

### Определение 1

**Операция** — это функция  $X_1 \times \dots \times X_n \rightarrow X$ .

Чаще всего рассматривается ситуация, когда  $X_1 = \dots = X_n = X$ . В этом случае операция называется *n-арной* операцией на множестве  $X$ .

*Пример 1.* 0-арная операция это выбор фиксированного элемента

### Определение 2

1-арная операция обычно называется **унарной** операцией

*Пример 2.*  $f : \mathbb{Z} \rightarrow \mathbb{Z} : f(n) = -n$  — унарная операция

### Определение 3

2-арная операция обычно называется **бинарной** операцией.

*Бинарные* операции обычно обозначаются не буквами, а значками, например  $\star$ , и вместо  $\star(x, y)$  пишут  $x \star y$ .

*Пример 3.*  $+: \mathbb{Z} \rightarrow \mathbb{Z} : +(a, b) = a + b$  — бинарная операция

### Определение 4

Пусть  $X$  — множество, а  $\star$  — бинарная операция на  $X$ . Определим следующие свойства.

(1)  $\forall x, y, z \in X : (x \star y) \star z = x \star (y \star z)$  — **ассоциативность**.

(2)  $\exists e \in X \forall x \in X : e \star x = x \star e = x$  ( $e$  называется **нейтральным элементом**).

(3)  $\forall x \in X \exists x' \in X : x \star x' = x' \star x = e$  ( $x'$  называется элементом **обратным** к  $x$ ).

Если выполнено только одно из равенств  $x' \star x = e$  или  $x \star x' = e$ , то  $x'$  называют левым или, соответственно, правым обратным к  $x$ .

(4)  $\forall x, y \in X : x \star y = y \star x$  — **коммутативность**.

*Пример 4.*  $\circ$  (композиция) на множестве параллельных переносов — ассоциативна

*Пример 5.* 0 — нейтральный элемент по сложению на множестве целых чисел

*Пример 6.* 2 обратный элемент к 3 на множестве остатков по модулю 5 с операцией умножения (с операцией сложения, кстати, тоже)

### Определение 5

Множество  $X$  с операцией  $\star$  называется

**полугруппой**, если операция ассоциативна;

**моноидом**, если операция ассоциативна и существует нейтральный элемент;

**группой**, если выполнены свойства (1) – (3)

Группа называется **Абелева**, если выполнено (4).

*Пример 7.* Группой является множество целых чисел с операцией сложения. Нейтральным элементом является 0, обратным элементом к  $x$  является  $-x$ . Группа коммутативна (Абелева).

*Пример 8.* Моноидом является множество целых чисел с операцией умножения. Нейтральным элементом является 1.

### Задача 1

Какие из множеств с бинарной операцией являются *группами*?

- $(\mathbb{N}, +)$
- $(\mathbb{Q}, +)$
- Параллельные переносы на плоскости с композицией
- $(\mathbb{Z}, \cdot)$
- $(\mathbb{Q}, \cdot)$
- Гомотетии на плоскости с композицией
- $(\mathbb{R}, +)$
- $(\mathbb{R}, \cdot)$
- Повороты квадрата с композицией

### Задача 2

*Нейтральный элемент* единственен (это утверждение не зависит даже от ассоциативности).

### Задача 3

Если элемент моноида имеет левый и правый обратный, то они совпадают. В частности, обратный элемент единственен.

### Задача 4

Если в моноиде элементы  $x$  и  $y$  обратимы, то  $x \star y$  обратим, причем  $(x \star y)^{-1} = y^{-1} \star x^{-1}$ . Множество обратимых элементов моноида является *группой*.

### Задача 5

Пусть  $G$  — группа относительно операции  $\circ$ . Операцию  $*$  определим так:  $a * b = b \circ a$ . Доказать, что относительно  $*$  множество  $G$  также является группой (противоположной группой).

### Задача 6

Пусть  $G$  — конечное множество с ассоциативной бинарной операцией, причем из  $ax_1 = ax_2$  следует  $x_1 = x_2$ , а из  $y_1a = y_2a$  следует  $y_1 = y_2$  при любом  $a \in G$ . Доказать, что  $G$  — группа.

### Задача 7

Доказать, что непрерывные строго возрастающие вещественные функции  $f$ , определенные на отрезке  $[0, 1]$  и имеющие значения  $f(0) = 0$  и  $f(1) = 1$ , образуют группу относительно суперпозиции.

### Определение 6

Определим **таблицу Кэли**, как квадратную таблицу, описывающую структуру конечной алгебраической системы и состоящая из результатов применения бинарной операции к её элементам.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Таблица 1: Таблица Кэли для остатков по модулю 3 с операцией сложения

Пример 9.

### Задача 8

Построить таблицу Кэли: (1) группы  $S$  биекций множества из  $n$  элементов относительно композиции (симметрической группы степени  $n$ ) для  $n = 3$ , (2) группы  $D$  самосовмещений правильного  $n$ -угольника относительно композиции для  $n = 3$ .

**Определение 7**

Пусть  $G$  с операцией  $\star$  и  $H$  с операцией  $\#$  – группы. Функция  $f : G \rightarrow H$  называется **гомоморфизмом**, если  $f(a \star b) = f(a) \# f(b)$  для любых  $a, b \in G$ .

Если **гомоморфизм** является биекцией, то его называют **изоморфизм**.

*Пример 10.* Рассмотрим множество целых чисел  $\mathbb{Z}$  с операцией сложения и множество всех степеней пятерок  $A = \{\dots 5^{-1}, 1, 5, 5^2, 5^3, \dots\}$  с операцией умножения. Тогда есть гомоморфизм  $f : \mathbb{Z} \rightarrow A$ .  $f(x) = 5^x$  Нетрудно проверить, что  $f(a + b) = f(a) \cdot f(b)$

*Пример 11.* Рассмотрим множество целых чисел  $\mathbb{Z}$  с операцией сложения и множество состоящее из 0 и 1 с операцией сложения (будем обозначать его  $\mathbb{F}_2$ ). Тогда есть гомоморфизм  $f : \mathbb{Z} \rightarrow \mathbb{F}_2$ .  $f(x) = x \bmod 2$  Нетрудно проверить, что  $f(a + b) = f(a) + f(b)$

**Задача 9**

Опишите все возможные группы состоящие из 1, 2 и 3 элементов с точностью до изоморфизма

**Задача 10**

- Докажите, что множество остатков по модулю 6 с операцией сложения является группой.
- Докажите, что множество остатков по модулю 7 за исключением 0 с операцией умножения является группой.

**Задача 11**

Докажите, что две группы из прошлого задания изоморфны.

**Задача 12**

Опишите все возможные группы состоящие из четырёх элементов с точностью до изоморфизма

**Задача 13 \***

Опишите все возможные группы состоящие из пяти элементов с точностью до изоморфизма

**Определение 8**

Непустое подмножество  $H$  группы  $G$  называется *подгруппой*, если  $a, b \in H \Rightarrow ab, a^{-1} \in H$ .

*Пример 12.* Если  $a \in H$ , то  $a^{-1} \in H$ , а, следовательно, и их произведение, равное нейтральному элементу, лежит в подгруппе  $H$ . Ясно, что подгруппа сама является группой относительно тех же операций, которые заданы в объемлющей группе. Если  $H$  – подгруппа в  $G$ , то пишут  $H \leq G$ .

*Пример 13.* В любой группе есть две тривиальные подгруппы: сама группа и множество, состоящее из одного нейтрального элемента.

*Пример 14.* Во множестве целых чисел с операцией сложения есть подгруппа чисел делящихся на 3.  $3\mathbb{Z} \leq \mathbb{Z}$ .

**Определение 9**

Пусть  $X$  — подмножество группы  $G$ . *Подгруппой, порожденной* множеством  $X$ , называется наименьшая подгруппа в  $G$ , содержащая  $X$ .

Подгруппа, *порожденная*  $X$ , обозначается  $\langle X \rangle$ .

Подгруппа, *порожденная* одним элементом (точнее, одноэлементным множеством) называется *циклической*.

**Теорема 1**

Любая циклическая группа изоморфна аддитивной группе  $\mathbb{Z}$  или  $\mathbb{Z}/n\mathbb{Z}$ .

**Определение 10**

Пусть  $G$  — группа. Количество элементов в этой группе называется *порядком группы*  $G$  и обозначается  $|G|$ .

**Определение 11**

Пусть  $g$  — элемент группы  $G$ . *Порядок циклической подгруппы*, порожденной  $g$ , называется *порядком элемента*  $g$ , т.е.  $\text{ord}_g = |\langle g \rangle|$ . *Порядок элемента*  $g$  — это наименьшее натуральное число  $n$  такое, что  $g^n = 1$ .

**Определение 12**

Пусть  $H \leq G$ . Множества  $gH$  и  $Hg$  называются левыми (соответственно правыми) **смежными классами** по подгруппе  $H$ .

Множество левых смежных классов обозначается через  $G/H$ , а правых —  $H \backslash G$ .

**Теорема 2 (Лагранж)**

Если  $H$  — подгруппа конечной группы  $G$ , то  $|G| = |H| \cdot |G/H|$ .

*Пример 15.* Если  $H$  — подгруппа конечной группы  $G$ , то в частности  $|G| : |H|$ .

**Задача 14**

Докажите, что  $\forall a \in G$  выполнено тождество  $a^{|G|} = e$ .

**Задача 15**

Докажите, что для каждого простого числа  $p$  группа состоящая из  $p$  элементов существует и единственна с точностью до изоморфизма.

**Задача 16**

Доказать, что в группе чётного порядка найдётся ненейтральный элемент с единичным квадратом.

**Задача 17**

Пусть  $G$  — группа относительно операции  $\circ$ ,  $a \in G$ . Определим на  $G$  новую операцию:  $x * y = x \circ a \circ y$ . Доказать, что относительно операции  $*$  множество  $G$  также является группой, и что новая группа изоморфна старой.

**Задача 18 \***

Доказать, что если в мультипликативно записанной группе квадрат любого элемента равен 1, то эта группа — абелева.

**Определение 13**

Пусть теперь на множестве  $R$  заданы операции «сложения» и «умножения», причем  $R$  является абелевой группой по сложению и полугруппой по умножению. Предположим, что выполнено следующее свойство:

(5)  $\forall x, y, z \in R : (x + y)z = xz + yz$  и  $z(x + y) = zx + zy$  (правая и левая дистрибутивность).

Тогда  $R$  называется **(ассоциативным) кольцом**. Если существует нейтральный элемент по умножению, то кольцо называется **кольцом с единицей**, если умножение коммутативно, то **коммутативным кольцом**.

*Пример 16.* Множество целых чисел с операцией сложения и умножения. По сложению это *Абелева группа*. По умножению есть 1. Так что это коммутативное кольцо с 1.

**Определение 14**

Как следует из задания 4, множество обратимых (по умножению) элементов кольца  $R$  является группой. Эта группа называется **мультипликативной подгруппой кольца** и обозначается через  $R^\times$ .

*Пример 17.* Мультипликативная подгруппа кольца  $\mathbb{Z}/12\mathbb{Z}$  это  $\{1, 5, 7, 11\}$  с операцией умножения по модулю 12.

**Задача 19**

Для любого элемента  $r$  произвольного кольца  $R$ :  $0 \cdot r = r \cdot 0 = 0$ . Если  $R$  – кольцо с единицей, то  $(-1) \cdot r = -r$ .

**Задача 20**

Сколько элементов в мультипликативной подгруппе кольца  $\mathbb{Z}/n\mathbb{Z}$

**Задача 21**

Докажите **теорему Эйлера** с помощью *теоремы Лагранжа*.

**Определение 15**

**Поле** – это коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим.

Пример 18.  $\mathbb{Q}, \mathbb{R}$  — поля

Пример 19. Через  $\mathbb{Z}/n\mathbb{Z}$  будем обозначать кольцо остатков по модулю  $n$  со стандартными операциями.

### Задача 22

Докажите, что  $\mathbb{Z}/n\mathbb{Z}$  — поле  $\iff n$  — простое

### Определение 16

Подгруппа  $H$  группы  $G$  называется **нормальной**, если для любых  $g \in G$  и  $h \in H$  имеет место включение  $g^{-1}hg \in H$ .

В других обозначениях:  $\forall g \in G : g^{-1}Hg \subseteq H$ . Если  $H$  — нормальная подгруппа в  $G$ , то пишут  $H \trianglelefteq G$ .

Пример 20. Заметим, что любая подгруппа абелевой группы является *нормальной*.

### Задача 23

Докажите, что у *нормальной подгруппы* левые и правые классы смежности равны и наоборот.

$\forall g \in G : gH = Hg \iff H$  — нормальная подгруппа.

### Задача 24

Приведите пример группы и её подгруппы, которая не является *нормальной*.

### Задача 25

Пусть  $H \trianglelefteq G$ .

Докажите, что  $G/H$  — тоже группа с индуцированной операцией

$$g_1H * g_2H = (g_1 * g_2)H$$

### Задача 26

Пусть  $H \leq G$  и  $|G| = 2|H|$ . Тогда  $H \trianglelefteq G$ .



**Задача 27**

Отображение  $\pi : G_1 \times G_2 \rightarrow G$  является изоморфизмом тогда и только тогда, когда

- (1)  $xy = yx$  при всех  $x \in G_1$  и  $y \in G_2$ .
- (2)  $G = G_1 G_2$ .
- (3)  $G_1 \cap G_2 = 1$ .

**Задача 28 \***

Найти все (с точностью до изоморфизма) группы порядка  $2p$ , где  $p$  — простое число.